UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/685,882	10/15/2003	Vincent J. Zimmer	INTEL/17849	5946

34431 7590 01/11/2007

HANLEY, FLIGHT & ZIMMERMAN, LLC
150 S. WACKER DRIVE
SUITE 2100
CHICAGO, IL 60606

EXAMINER	
MORAN, RANDAL D	
ART UNIT	**PAPER NUMBER**
2135	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/11/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/685,882	ZIMMER ET AL.	
	Examiner	**Art Unit**	
	Randal D. Moran	2196	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 October 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *15 October 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *11/3/2003 and 8/16/2006*.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. The Information Disclosure Statement's filed on 11/3/2003 and 8/16/2006 have been considered by the examiner.

2. Claims 1-29 are pending in this application.

Claim Objections

3. Claim 3 is objected to because of the following informalities:

- Claim 3, line 3- "chassis associated of the processor system" contains a grammatical error. Appropriate correction is required.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

5. **Claims 1, 2, 7-9, 13, 15, 16, 21-24, and 29,** are rejected under 35 U.S.C. 102(a) as being anticipated by **Mitchem, T.; Lu, R.; O'Brien, R.; Using Kernel Hypervisors to Secure Applications, IEEE, Dec. 1997 Page(s): 175 – 181**, herein after "Mitchem."

6. Considering **Claim 1,** Mitchem discloses a method to provide network traffic support and physical security support (p.175 right column, lines 2-6) comprising: initializing a virtual machine monitor (VMM) in a processor system during a pre-boot phase (p. 175 left column, ¶ 4, lines 4-7, right column, lines 6-8, loadable modules that perform pre-call processing would be initiated in a pre-boot/pre-load phase); identifying at least one of a network traffic intrusion event and a physical security intrusion event with the VMM (p.179 left column, Client Kernel Hypervisors, ¶ 2 lines 3-9, p.180 right column, Fine Grained Access Control, lines 1-18); and implementing at least one of a network traffic support and a physical security support in response to the at least one of the network traffic intrusion event and the physical security intrusion event (p.179 left column, Client Kernel Hypervisors, ¶ 2 lines 6-9, p.180 right column, Fine Grained Access Control, lines 1-18).

7. Considering **Claim 8,** Mitchem discloses a machine readable medium storing instructions, which when executed, cause a machine to (p.175 right column, lines 6-8): initialize a virtual machine monitor (VMM) in a processor system during a pre-boot phase (p. 175 left column, ¶ 4, lines 4-7, right column, lines 6-8, loadable modules that perform pre-call processing would be initiated in a pre-boot/pre-load phase); identify at least one of a network traffic intrusion event and a physical security intrusion event with the VMM (p.179 left column, Client Kernel

Hypervisors, ¶ 2 lines 3-9, p.180 right column, Fine Grained Access Control, lines 1-18); and implement at least one of a network traffic support and a physical security support in response to detecting the at least one of the network traffic intrusion event and the physical security intrusion event (p.179 left column, Client Kernel Hypervisors, ¶ 2 lines 6-9, p.180 right column, Fine Grained Access Control, lines 1-18).

8. Considering **Claim 15,** Mitchem discloses an apparatus to provide network traffic support and physical security support comprising (p. 175 left column, ¶ 4, line 4-7): a data structure configured to store firmware of a processor system (p.175 right column, lines 6-8); and a virtual machine monitor initialized from the firmware during a pre-boot phase (p. 175 left column, ¶ 4, lines 4-7, right column, lines 6-8, loadable modules that perform pre-call processing would be initiated in a pre-boot/pre-load phase) to identify at least one of a network traffic intrusion event and a physical security intrusion event (p.179 left column, Client Kernel Hypervisors, ¶ 2 lines 3-9, p.180 right column, Fine Grained Access Control, lines 1-18), and to implement at least one of a network traffic support and a physical security support in response to detecting the at least one of the network traffic intrusion event and the physical security intrusion event (p.179 left column, Client Kernel Hypervisors, ¶ 2 lines 6-9, p.180 right column, Fine Grained Access Control, lines 1-18).

9. Considering **Claim 23,** Mitchem discloses a processor system to provide network traffic support and physical security support (p. 175 left column, ¶ 4, line 4-7) comprising: flash memory configured to store code associated with a virtual machine monitor (VMM) of the processor system (p.175 right column, lines 6-8); and a processor operatively coupled to the flash memory (p. 175 left column, ¶ 4, lines 4-7, p. 175 right column, lines 6-8); the processor being programmed to initialize the VMM during a pre-boot phase (p. 175 left column, ¶ 4, lines 4-7), to identify at least one of a network traffic intrusion event and a physical security intrusion event with the VMM (p.179 left column, Client Kernel Hypervisors, ¶ 2 lines 3-9, p.180 right column, Fine Grained Access Control, lines 1-18), and to implement at least one of a network traffic support and a physical security support in response to the at least one of the network traffic intrusion event and the physical security intrusion event (p.179 left column, Client Kernel Hypervisors, ¶ 2 lines 6-9, p.180 right column, Fine Grained Access Control, lines 1-18).

10. Considering **Claims 2, 9, 16, and 24,** Mitchem discloses identifying the at least one of the network traffic intrusion event and the physical security intrusion event with the VMM comprises detecting at least one of a packet accessing a restricted port, a packet associated with a virus identifier, a SYN packet, and an alert standard format packet (p.179 left column, Client Kernel Hypervisors, ¶ 2 lines 3-9, monitoring system calls made by the browser and enforcing a policy that only

allowed certain resources to be accessed reads on detecting a packet accessing a restricted port, p.180 right column, Fine Grained Access Control, lines 1-18).

11. Considering **Claims 7, 13, 22, and 29,** Mitchem discloses the processor system is associated with at least one of a private internal network and the Internet (p. 179 left column, Client Kernel Hypervisors, ¶ 2 lines 2-6).

12. Considering **Claim 21,** Mitchem discloses the data structure comprises a flash memory (p.175 right column, lines 6-8).

13. **Claims 4, 11, 19, and 27** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Mitchem**.

14. Considering **Claims 4, 11, 19, and 27,** Mitchem does not explicitly disclose implementing the at least one of the network traffic support and the physical security support comprises discarding a packet associated with network traffic in response to identifying the network traffic intrusion event.

Official notice is taken that it would have been obvious to one of ordinary skill in the art to discard a packet attempting to access a restricted port. Discarding the packet would have been the most logical and efficient action to be taken.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Mitchem by discarding the packet attempting to access the restricted port for the benefit of not allowing the packet into areas it is not authorized to be in.

Claim Rejections - 35 USC § 103

15. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

16. **Claims 3, 5, 6, 10, 12, 17, 18, 20, 25, 26, and 28** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Mitchem** in view of **Klein et al. (US 6,134,665)**, herein after "Klein."

17. Considering **Claims 3, 10, 17, 18, 25, and 26** Mitchem does not disclose identifying the at least one of the network traffic intrusion event and the physical security intrusion event with the VMM comprises detecting opening of a chassis associated of the processor system via a chassis intrusion switch.

Klein does disclose identifying the at least one of the network traffic intrusion event and the physical security intrusion event with the VMM comprises detecting opening of a chassis associated of the processor system via a chassis intrusion switch (column 19 lines 66-67, column 20 lines 1-5).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Mitchem by the chassis intrusion switch as taught by Klein in order to inform proper authorities that the failure has occurred. Hardware, such as power supply voltage, fan operation, chassis intrusion, etc. can be detected directly by appropriate sensors. In the event that any component fails, the inventive computer system transmits a message onto the network in order to inform proper authorities that the failure has occurred (Klein- column 19 lines 28-35)

18. Considering **Claims 5, 12, 20, and 28,** Mitchem does not disclose implementing the at least one of the network traffic support and the physical security support comprises disabling the processor system in response to identifying the physical security intrusion event.

Klein does disclose implementing the at least one of the network traffic support and the physical security support comprises disabling the processor system in response to identifying the physical security intrusion event (column 19 lines 66-67, column 20 lines 1-5).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Mitchem by the ability to disable the processor in response to identifying the physical security intrusion event as taught by Klein in order to prevent unauthorized use of the system.

19. Considering **Claim 6,** Mitchem does not disclose identifying a user authorization for the physical security intrusion event of the processor system.

Klein does disclose identifying a user authorization for the physical security intrusion event of the processor system (column 19 lines 66-67, column 20 lines 1-5, sending an alarm message to the system manager would be one technique for determining user authentication).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Mitchem by identifying a user authorization for the physical security intrusion event as taught by Klein in order to prevent unauthorized use of the system.

20. **Claim 14** is rejected under 35 U.S.C. 103(a) as being unpatentable over **Mitchem** in view of **Rawson (US 2004/0111596)**.

21. Considering **Claim 14,** Mitchem does not specifically disclose the machine readable medium comprises one of a programmable gate array, application specific integrated circuit, erasable programmable read only memory, read only memory, random access memory, magnetic media, and optical media.

Rawson does disclose the machine readable medium comprises one of a programmable gate array, application specific integrated circuit, erasable programmable read only memory, read only memory, random access memory, magnetic media, and optical media ([0027]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Mitchem by the machine readable medium comprising one of a programmable gate array, application specific integrated circuit, erasable programmable read only memory, read only memory, random access memory, magnetic media, and optical media as taught by Rawson for the benefit of partitioning a data processing system such as a multi-processor (SMP) server system into independent and logically distinct partitions (Rawson- [0027] lines 5-8).

Conclusion

22. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- US 6,795,926 - chassis intrusion switch
- US 2003/0163723 – virtual machine monitor
- US 5,835,726 – virtual machine security functions

23. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Randal D. Moran whose telephone number is 571-270-1255. The examiner can normally be reached on M-F: 7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nabil El-Hady can be reached on 571-272-3963. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Randal D. Moran
RDm
1/7/07

ANDREW Y. KOENIG
PRIMARY PATENT EXAMINER